التاريخ:
31 مارس 2008
(نص مُنقَّح)

اللغة العربية

تقرير مشاكل GNSO حول استضافة التمويه السريع

حالة هذه الوثيقة

هذه الوثيقة عبارة عن تقرير مشاكل حول استضافة التمويه السريع الذي طلبه مجلس GNSO.

ملاحظة حول الترجمات

كُتبت النسخة الأصلية لهذه الوثيقة باللغة الإنجليزية، وهي متاحة على
http://gnso.icann.org/issues/fast-flux-hosting/gnso-issues-report-fast-flux-25mar08.pdf.

وأينما وجد اختلاف في المعنى أو ما يوهم أنه اختلاف في المعنى بين هذه الوثيقة والنص الأصلي، فسيكون النص الأصلي هو السائد.

ملخص

تم تقديم هذا التقرير إلى مجلس GNSO في استجابة لطلب من المجلس نتيجة لاقتراح تم اقتراحه ودعمه أثناء اجتماع المجلس من خلال تقنية متابعة المؤتمرات عن بعد في 6 مارس 2008.

وتم تقديم التقرير إلى مجلس GNSO لأول مرة في 25 مارس. وتم استبدال الوثيقة السابقة بهذا التقرير.

التاريخ:
31 مارس 2008
(نص مُنقَّح)

اللغة العربية

جدول المحتويات

التاريخ:
31 مارس 2008
(نص مُنقَّح)

اللغة العربية

التاريخ:
31 مارس 2008
(نص مُنقَّح)

اللغة العربية

1 ملخص تنفيذي

خلفية

انتهت اللجنة الاستشارية للأمان والاستقرار (SSAC) التابعة لـ ICANN مؤخرًا من دراسة تتعلق بكيفية التلاعب بـ DNS بواسطة مجرمي الإنترنت الإلكترونيين لتجنب اكتشافهم والقضاء على أنشطتهم غير القانونية. وتم نشر نتائج الدراسة في يناير 2008 في *تقرير SSAC الاستشارية حول استضافة التمويه السريع وDNS* (SAC 025)[1]، والذي يصف التقنيات التي تمت الإشارة إليها إجمالاً بـ "استضافة التمويه السريع"، وهي توضح كيفية تمكين هذه التقنيات المجرمين الإلكترونيين من إطالة مدة الاستمرار المفيدة للمضيفين المشبوهين بشكل ضار في أنشطة غير قانونية، و"تشجيع ICANN وأصحاب السجلات والمُسجلون...لوضع أفضل الممارسات لتخفيف استضافة التمويه السريع، والبحث فيما إذا كان من الضروري تناول هذه الممارسات في اتفاقيات [الاعتماد] المستقبلية". [2]

وقد قام مجلس GNSO -أثناء اجتماعه المُقام من خلال تقنية متابعة المؤتمرات عن بعد في 6 مارس 2008[3]- بمناقشة الاقتراح التالي الذي يتضمن في محتواه:

> "ينبغي على موظفي ICANN إعداد تقرير مشاكل فيما يتعلق بتغييرات "التمويه السريع" لـ DNS، بهدف قيام مجلس GNSO بدراسته. وبشكل أكثر تحديداً، ينبغي على الموظفين مراعاة تقرير SAC الاستشارية [SAC 025]، وتوضيح الخطوات التالية المحتملة في تطوير سياسة GNSO والتي تم وضعها لخفض القدرة الحالية للمجرمين على استغلال DNS عبر "التمويه السريع" لعنوان بروتوكول الإنترنت (IP) أو تغييرات خوادم الأسماء".

وفي استجابة لهذا الطلب، قام موظفو ICANN بمناقشة تقرير SAC الاستشارية (SAC 025)، كما قاموا بالتشاور مع مصادر المعلومات الأخرى المناسبة ذات الصلة حول موضوع استضافة التمويه السريع.

تعريفات

التمويه السريع.

---

[1] http://www.icann.org/committees/security/sac025.pdf
[2] على الرغم من إشارة التقرير (SAC 025) فقط إلى "الاتفاقيات"، غير أن العرض التقديمي الذي تقدمت به SSAC حول التمويه السريع في فبراير 2008 في دلهي (http://delhi.icann.org/files/presentation-rasmussen-fast-flux-13feb08.pdf) قد أوضح أن المرجع المقصود هو "اتفاقيات الاعتماد".
[3] http://gnso.icann.org/meetings/agenda-06mar08.shtml

الكاتب: ليز جاستر، policy@icann.org

يُشير مصطلح "التمويه السريع" في هذا السياق إلى التغييرات السريعة والمتكررة في سجلات مورد A و/أو NS الموجودة في منطقة DNS، والتي تتمتع بتأثير إحداث تغير سريع في الموقع (عنوان بروتوكول الإنترنت (IP)) الذي يتم تحويل اسم نطاق مُضيف الإنترنت (A) أو خادم الاسم (NS) إليه.

التمويه الفردي

هو نوع مختلف من التمويه السريع حيث تؤدي التحديثات السريعة في سجلات A الموجودة في ملف المنطقة الخاص بنطاق فرعي (ويكون عادةً من المستوى الثاني أو الثالث) إلى تغير سريع في الموقع (عنوان بروتوكول الإنترنت (IP)) الخاص بمضيفي الإنترنت (مثل، مواقع الويب أو خوادم المحتوى الأخرى).

تمويه خادم الاسم

هو نوع مختلف من التمويه السريع حيث تؤدي التحديثات السريعة في سجلات NS الموجودة في ملف المنطقة الخاص بأحد نطاقات المستوى الأعلى إلى تغير سريع في موقع (عنوان بروتوكول الإنترنت (IP)) خادم/خوادم الاسم الخاص بنطاق فرعي واحد أو أكثر.

التمويه المزدوج

هو نوع مختلف من التمويه السريع حيث يتم استخدام كل من التمويه الفردي وتمويه خادم الاسم لإحداث تغير سريع في كل من المضيفين وخوادم الاسم.

استضافة التمويه السريع

هو ممارسة استخدام تقنيات التمويه السريع لإخفاء مكان مواقع الويب أو خدمات الإنترنت الأخرى التي تستضيف أنشطة غير قانونية.

شبكة خدمة التمويه السريع

هي شبكة تتكون من نظم الكمبيوتر المشبوهة ("botnets") باستخدام سجلات DNS عامة تتغير باستمرار.

توصيات الموظفين

لقد أدت المشاكل المتعلقة باستضافة التمويه السريع إلى عقد مناقشات هامة بين العديد من الدوائر الانتخابية وأصحاب المصالح، وستكون هناك فائدة من المزيد من البحث والمراجعة. ومن ثم، يوصي الموظفون بقيام GNSO برعاية عمليات إضافية لتحديد الحقائق والمعلومات وعمليات بحث لتطوير الإرشادات المتعلقة بتنفيذ أفضل الممارسات قبل تحديد ما إذا كان سيتم بدء عملية رسمية لتطوير السياسة أم لا. وستتم إتاحة موارد الموظفين لدعم هذه الأنشطة البحثية والأهداف. ويُرحب موظفو ICANN بالتوجيهات الخاصة باتجاهات محددة لمزيد من البحث، بهدف مساعدة المجتمع في عملية صنع القرار.

وعلى الرغم من احتمال قيام GNSO بإقرار البدء، غير أن الموظفين يُشيرون إلى أهمية إكمال عمليات تحديد الحقائق والمعلومات وعمليات بحث في مداولات المجتمع.

وفي إطار تحديد ما إذا كانت المشكلة تقع داخل نطاق عملية سياسة ICANN ونطاق GNSO، قام الموظفون ومكتب المجلس العام بمناقشة العناصر التالية:

- تحديد ما إذا كانت المشكلة تقع داخل نطاق إعلان مهمة ICANN،
- تحديد ما إذا كان من الممكن تطبيق المشكلة بشكل واسع على عدد من الأوضاع والمنظمات المتعددة،
- تحديد ما إذا كان من المحتمل استمرار قيمة المشكلة أو سريانها، على الرغم من الحاجة إلى إجراء تحديثات أحيانًا،
- تحديد ما إذا كانت المشكلة ستؤدي إلى وضع دليل أو إطار عمل لصنع القرار في المستقبل، و
- تحديد ما إذا كانت المشكلة تتضمن إحدى سياسات ICANN الحالية أو تؤثر عليها.

وبناءً على ما سبق، يرى المجلس العام وجود بعض النواحي المتعلقة بموضوع استضافة التمويه السريع داخل نطاق عملية سياسة ICANN ونطاق GNSO. ومع ذلك، يُشير المجلس العام أيضًا إلى أن السؤال الإجمالي حول كيفية تخفيف استخدام استضافة التمويه السريع في الجريمة الإلكترونية أوسع من عملية تطوير سياسة GNSO. ولن يتم تطبيق بعض الخطوات التي يمكن استخدامها لعدم تشجيع استضافة التمويه السريع أو إعاقتها، مثل الخطوات التي يمكن اتخاذها من قِبل ccTLDs أو مقدمي خدمات الإنترنت أو مستخدمي الإنترنت أنفسهم داخل نطاق وضع سياسة GNSO. ويتم استهداف النطاقات الموجودة

في ccTLDs أيضًا. وبالإضافة إلى ذلك، يُعد السؤال الخاص بإمكانية أن تكون خيارات السياسة ذات "قيمة مستمرة أو سارية" ذا أهمية خاصة في سياق استضافة التمويه السريع، حيث من الممكن تقويض قواعد ثابتة تم فرضها عبر عملية تطوير السياسة بشكل سريع بواسطة المجرمين الإلكترونيين الجسورين.

وبناءً على المعلومات المتوفرة حتى الوقت الحالي، يقترح الموظفون دراسة الخيارات المحتملة لتطوير السياسة بشكل أكثر تفصيلاً. وستُوفر عمليات تحديد الحقائق الإضافية عمليات الاطلاع الضرورية لإخبار المجلس بشكل أفضل بخيارات السياسة التي قد تكون أكثر فعالية. ويمكن أن تُوفر الخيارات المُفضَّلة بعد ذلك أساسًا لبدء تشغيل عملية محددة لتطوير السياسة.

2 الهدف

تم تقديم هذا التقرير في استجابة لطلب من مجلس GNSO الخاص بتقديم "تقرير مشاكل حول استضافة التمويه السريع".

وفي هذا السياق، وبالتوافق مع متطلبات لوائح ICANN:

أ. الموضوع المُقترَح الذي تمت إثارته للمناقشة هو استضافة التمويه السريع.
ب. مجلس GNSO هو مُمثِّل الطرف التي قام بتقديم المشكلة.
ج. مدى تأثير المشكلة على هذا الطرف: تُعد GNSO هي المسؤولة عن تطوير السياسة المتعلقة بنطاقات المستوى الأعلى العامة. وتقوم استضافة التمويه السريع كثيرًا باستهداف gTLDs (وذلك على الرغم من ملاحظة ذلك أيضًا في ccTLDs)، كما تهتم GNSO بأنشطة الخداع والتحايل وأنشطة الإجرام الإلكتروني الأخرى التي يمكن أن تؤدي إلى خفض استقرار تشغيل الإنترنت وأمانه والتي يتم تسهيلها من خلال تقنيات قد تقع داخل نطاق مسؤوليات وضع سياسة GNSO.
د. دعم المشكلة لبدء تشغيل عملية تطوير السياسة (PDP): تم إظهار دعم كاف لتجهيز تقرير المشاكل هذا أثناء اجتماع مجلس GNSO المُقام من خلال تقنية متابعة المؤتمرات عن بعد في 6 مارس 2008. وكانت نتيجة التصويت تأييد 10 أصوات لتطوير تقرير مشاكل مقابل رفض 14 صوتًا. وطبقًا للوائح ICANN، يمكن إثارة أية قضية للمناقشة كجزء من عملية تطوير السياسة (PDP) "من خلال تصويت 25% على الأقل من أعضاء المجلس الحاضرين...".

3 خلفية

يُشير "التمويه السريع" إلى التغييرات السريعة والمتكررة في سجلات مورد A و/أو NS الموجودة في منطقة DNS، والتي تتمتع بتأثير إحداث تغير سريع في الموقع (عنوان بروتوكول الإنترنت (IP)) الذي يتم تحويل اسم نطاق مُضيف الإنترنت (A) أو خادم الاسم (NS) إليه. وعلى الرغم من وجود بعض الاستخدامات القانونية المُعترَف بها لهذه التقنية (انظر أدناه)، غير أنه تم استخدامها على مدار العام الماضي كأداة مُفضَّلة للمحتالين والمجرمين الإلكترونيين الآخرين الذين يقومون باستخدامها لتجنب الكشف من جانب محققي مكافحة الجريمة.

كيف يعمل التمويه السريع[4]

إن الهدف من التمويه السريع هو حصول اسم نطاق مُؤهَّل تأهيلاً كاملاً (مثل www.example.com) على عناوين بروتوكول إنترنت (IP) متعددة (مئات أو حتى آلاف) تم تخصيصها له. ويتم تغيير عناوين بروتوكول الإنترنت (IP) هذه داخل ملف منطقة A (عنوان المضيف) وخارجه و/أو سجلات NS (خادم الاسم) مع تكرار شديد، باستخدام مجموعة من عناوين بروتوكول الإنترنت الدوارة ومدة استمرار (TTL) قصيرة جدًا. قد ترتبط أسماء مضيف موقع الويب بمجموعة جديدة من عناوين بروتوكول الإنترنت (IP) والتي يمكن تغييرها بشكل سريع. ويمكن في الحقيقة توصيل المتصفح الذي يتم توصيله بنفس موقع الويب بشكل متكرر خلال فترة زمنية قصيرة بجهاز كمبيوتر مصاب مختلف في كل مرة. وبالإضافة إلى ذلك، يتأكد المعتدون من وجود أفضل سعة نطاق ومستوى توافر الخدمة الممكنين في النظم المشبوهة التي يستخدمونها في استضافة أعمال الاحتيال الخاصة بهم. ويقومون كثيرًا باستخدام مخطط لتوزيع الأحمال والذي يراعي نتائج الكشف عن الأجهزة المتصلة، حتى يمكن إخراج أية أجهزة غير مستجيبة من التمويه وتتم المحافظة دائمًا على تواجد المحتوى.

[4] تعتمد المادة الموجودة في هذا القسم على بعض الحالات المنقولة حرفيًا من الوصف الوارد على الموقع http://www.honeynet.org/papers/ff/fast-flux.html.

وتؤدي عمليات إعادة توجيه البروكسي إلى إضافة طبقة ثانية من التعتيم لمواجهة التمويه السريع. وعند قيام شخص ما باستضافة محتوى ضار (موقع احتيال، على سبيل المثال) يستخدم شبكة تمويه سريع، يكون المضيفون "المخدوعون" (من خلال التغير السريع في عنوان بروتوكول الإنترنت (IP) الذي يتم تحويل اسم النطاق إليه) بشكل نموذجي بمثابة البروكسي الذي يقوم بإعادة توجيه الاستفسارات إلى الموقع الذي يتضمن المحتوى الحقيقي للمعتدي. ويكون ذلك أمرًا سهلاً بالنسبة للمعتدي، حيث يمكنه وضع المحتوى الضار على مضيف واحد بدلاً من نسخه على العديد من botnets المختلفة، واستخدام botnets لإعادة توجيه البروكسي الذي يُشير إلى هذا المضيف. ثم يحدث التمويه بعد ذلك بين الموجِّهات. وتعمل إعادة التوجيه على تعطيل محاولات اكتشاف الأجهزة المتصلة بشبكة خدمة التمويه السريع وتخفيفها. ولن يتم الاستمرار في تحويل أسماء النطاق وعناوين URLs الخاصة بالمحتوى الذي يتم الإعلان عنه إلى عنوان بروتوكول الإنترنت (IP) الخاص بخادم محدد ولكنه يتردد بين العديد من الموجِّهات الأمامية أو البروكسي، والتي تقوم بدورها بتوجيه المحتوى إلى مجموعة أخرى من الخوادم الخلفية. وعلى الرغم من استخدام هذه التقنية لبعض الوقت في عالم عمليات تشغيل خوادم الويب القانونية بهدف المحافظة على درجة توفر عالية وتوزيع للحمل، غير أنه يكون في هذه الحالة دليلاً على التطور التقني لشبكات أجهزة الكمبيوتر الإجرامية.

"الناقلات الرئيسية" للتمويه السريع هي عناصر التحكم في شبكات خدمة التمويه السريع، وتُشبه نظم القيادة والتحكم (C&C) الموجودة في botnets التقليدية. ومع ذلك، ومقارنةً بالخوادم النموذجية لbotnets، تتمتع الناقلات الرئيسية للتمويه السريع بالعديد من المزايا الإضافية. وهي عبارة عن الجهاز المتصل بالجزء الأعلى من الناقلات الرئيسية للتمويه السريع، والذي يتم إخفاؤه من خلال أجهزة شبكات بروكسي التمويه السريع الأمامية المتصلة، والتي تعمل في الحقيقة على نقل المحتوى مرةً أخرى إلى العميل الضحية الذي يطلب هذا المحتوى. وتستخدم نظم قيادة وتحكم التمويه السريع المحددة تطبيقات النظير مقابل النظير (P2P) وبالتالي فإنها تعمل بنجاح في النظام على مدار فترات زمنية طويلة. وتتم ملاحظة استضافة هذه الأجهزة المتصلة لكل من خدمات DNS وHTTP في أحيان كثيرة، مع قدرة خادم الويب الذي يقوم ظاهريًا باستضافة عمليات التهيئة على إدارة درجة توفر المحتوى لآلاف من النطاقات بشكل فوري على مضيف واحد.

وتُعد شبكات التمويه السريع هي المسؤولة عن العديد من الممارسات الضارة، بما في ذلك متاجر الصيدليات عبر الإنترنت ومواقع إعادة توظيف الأموال ومواقع الاحتيال ومحتوى البالغين المتطرف/غير القانوني وبرامج تصفح الويب التي تقوم باستغلال مواقع الويب وتوزيع تنزيلات البرامج الضارة. ويمكن توصيل خدمات أخرى بخلاف DNS وHTTP مثل، SMTP وPOP وIMAP عبر شبكات خدمة التمويه السريع. ونظرًا لاستخدام التمويه السريع لعمليات إعادة توجيه TCP وUDP، قد يواجه أي بروتوكول خاص بخدمة توجيهية ذو منفذ هدف واحد بعض المشاكل الخاصة بالخدمة التي يتم تقديمها عبر شبكة خدمة التمويه السريع وبالتالي فهي ليست مجرد مواقع ويب، فقد تكون مواقع بريد إلكتروني محتالة.

الاستخدامات القانونية للتمويه السريع

يُدرك الموظفون -من خلال البحث التمهيدي- أن بعض نظم موازنة الحمل ذات السعة الكبيرة قد تعتمد على قيم مدة استمرار قصيرة في سجلات DNS التي تقوم بتحويل أسماء النطاقات الرئيسية لهذه السجلات (مثل www.google.com) إلى عناوين بروتوكول الإنترنت (IP) لنشر التغييرات بشكل سريع.[5] وقد يقوم أحد المواقع ذات الحركة المرتفعة باستخدام هذه التقنية - والتي تتلاءم مع تعريف "التمويه السريع"- لتعديل عناوين الصفحة الرئيسة الخاصة به لتتناسب مع أحوال الشبكة الداخلية والخارجية، مثل حمل الخادم وحالات التوقف وموقع المستخدم وإعادة تهيئة المورد. ونظرًا لأن الذاكرة الوسيطة لمعظم برامج التصفح تستغرق من 15 إلى 20 دقيقة على الأقل في عمليات بحث اسم نطاق -دون النظر إلى مدة الاستمرار (TTL) المُعلن عنها- فإن التأثير النهائي لمدة الاستمرار القصيرة (TTL) يساوي وضع زمن الانقضاء الفعلي الخاص بـ "حد الانتباه" لبرنامج التصفح. ويراعي مزودو هذه الخدمة القدرة على إعادة التهيئة بشكل سريع لتتمتع بالأهمية الكافية لإزاحة زمن انتظار الطلبات الإضافية الناتجة عن عمليات بحث DNS المتكررة. وتوجد حاجة إلى المزيد من البحث لفهم الاستخدامات القانونية وانتشارها بشكل أفضل.

ويدُرك الموظفون أيضًا إمكانية تمتُّع مزودو الخدمة بالقدرة على إحداث تمويه سريع لعناوين بروتوكول الإنترنت (IP) الخاصة بهم للتعامل مع الأوضاع التي تقوم فيها الحكومة أو أي وكيل آخر بشكل مدروس بحظر ("استبعاد") عناوينهم في محاولة لمنع الوصول إلى خدماتهم من داخل بلد محدد أو منطقة محددة. وتم ذكر ذلك على سبيل الحكاية كـ "استخدام قانوني" محتمل. وهذا هو مجال آخر حيث قد تكون هناك حاجة إلى فهم أفضل للمشاكل الفنية بهدف إجراء مناقشة أوسع.

سبب كون التمويه السريع بمثابة مشكلة

تُمثِّل الأنشطة الخداعية والمحتالة والأنشطة الضارة الأخرى (وكثيرًا ما تكون غير قانونية) تهديدًا معروفًا لسلامة مستخدمي الإنترنت وأمنهم. ويستطيع الأفراد المشتركون في هذه الأنشطة إحباط جهود المحققين في تحديد مواقع التشغيل الخاصة بهم وإغلاقها من خلال استخدام شبكات التمويه السريع لتغيير عناوين بروتوكول الإنترنت (IP) التي يستضيفها المحتوى الخاص بهم بشكل سريع ومستمر، مع الاستمرار في وضع "متقدم بخطوة واحدة" على مسؤولي تنفيذ القانون الذين يقومون بملاحقتهم.

[5] تقترح المعلومات التي حصل عليها الموظفون إلى أن مدة الاستمرار التي تصل إلى 300 ثانية قد تكون مطابقًا لما هو في عمليات التهيئة هذه. ومرةً أخرى، يجب إجراء المزيد من البحث للتحقق.

وتقوم شبكات خدمة التمويه السريع بتغيير سجلات DNS الخاصة بعنوان بروتوكول الإنترنت (IP) للجهاز الأمامي المتصل الخاص بهم بشكل متكرر في كل فترة زمنية من 3 إلى 10 دقائق، وبالتالي إذا تم إيقاف تشغيل أحد أجهزة موجه عامل التمويه المتصلة، يكون العديد من المضيفين المصابين الآخرين في وضع الاستعداد ومتاحين لتولي موضعه بسرعة. وتتكون شبكات التمويه السريع بشكل رئيسي من الأجهزة المنزلية المشبوهة، لأنه على عكس البنية التحتية لأجهزة الكمبيوتر الموجودة في الشركات أو المنظمات الأخرى التي يوجد بها قسم إدارة تكنولوجيا المعلومات، يكون من الصعب حماية أجهزة الكمبيوتر المنزلية باستخدام إجراءات مكافحة البرامج الضارة.

تقوم شبكات خدمة التمويه السريع بإنشاء بُنى أساسية قوية ومُعقدة لتوصيل الخدمة مما يُمثِّل صعوبة بالنسبة لمسؤولي النظم وعملاء تنفيذ القانون لإغلاق أعمال الاحتيال النشطة وتحديد المجرمين الذين يقومون بتشغيلها.

السبب الذي يدعو ICANN إلى الاهتمام بالتمويه السريع

استنتج مجتمع الباحثين ومسؤولي النظام ومسؤولي تنفيذ القانون وهيئات حماية المستهلك -الذين يقومون بمكافحة أعمال الاحتيال على الإنترنت التي يتم تمكينها أو زيادة سرعتها من خلال استضافة التمويه السريع- أن محاولة اعتراض استضافة التمويه السريع من خلال اكتشاف botnets وتفكيكها (شبكات خدمة التمويه السريع) ليست فعالة. ومن المتوقع أن تكون الإجراءات الأخرى التي تتطلب تعاون أصحاب سجلات DNS ومكاتب التسجيل لتحديد تقنيات التمويه السريع أو إلغائها أكثر فعالية. وينبغي على ICANN التفكير فيما إذا كانت ستقوم بتشجيع مُشغلي السجلات ومكاتب التسجيل وكيفية القيام بذلك لاتخاذ خطوات من شأنها المساعدة في خفض الخسائر الناتجة عن المجرمين الإلكترونيين وذلك من خلال خفض فعالية عمليات الاستغلال هذه التي تعتمد على DNS.

4 مناقشة الاتجاهات المحتملة

أكد البحث الذي قام موظفو ICANN بإجرائه على أن استضافة التمويه السريع:

- ظاهرة حقيقية - وتمت ملاحظتها وتوثيقها وتقديم تقارير خاصة بها من قِبل العديد من المصادر حسنة السمعة، بما في ذلك مجموعة عمل مكافحة الاحتيال،
- تُمثِّل مزيدًا من الصعوبة بالنسبة للمحققين لتحديد الأنشطة الضارة وإغلاقها، و
- يمكن خفض أنشطتها بشكل كبير من خلال إجراء تغييرات في طريقة التشغيل الحالية الخاصة بأصحاب سجلاتDNS ومكاتب التسجيل.

ونظرًا لتضمُّن استضافة التمويه السريع للعديد من الأطراف -المجرمون الإلكترونيون وضحاياهم وISPs والشركات التي توفر خدمات استضافة الويب ومزودو امتداد DNS والمُسجلون- من الممكن تصوُّر العديد من الطرق المختلفة للتهدئة. وتُحدد ورقة SSAC الاستشارية ثلاثة طرق للتهدئة، وتتطلب كل منها تعاون مجموعة مختلفة من الوكلاء:

- التخلص من botnets (المستخدمون وISPs)،
- تحديد مضيفي التمويه السريع وإغلاقها (ISPs) و
- تغيير طريقة تعامل أصحاب السجلات ومكاتب التسجيل مع تحديثات المنطقة، والتي قد تؤدي إلى خفض التمويه السريع أو تجعله غير جذاب (أصحاب السجلات ومكاتب التسجيل). وكما هو مُوضَّح بمزيد من التفصيل أدناه، توجد حاجة إلى المزيد من البحث والمناقشة لمعرفة فعالية العديد من الخيارات بمرور الوقت.

وقد قام خبراء مكافحة الجريمة الإلكترونية بإخبار الموظفين أن محاولة إيقاف عمليات الاحتيال والخداع الأخرى عبر الإنترنت من خلال التخلص من botnets هو أمر لا طائلة منه. حيث تتكون معظم botnets من أجهزة كمبيوتر مشبوهة تتصل بشبكات ذات سعة نطاق داخلية (على سبيل المثال، DSL أو كبل)، ويكون من السهل نشر البرامج الضارة بين هذه الأجهزة، وعلى الرغم من إمكانية تعاون مقدمي خدمة اللإنترنت في بعض البلدان في تحديد botnets والتخلص منها، يقوم بعض مقدمي خدمة اللإنترنت بتوفير "بيئة آمنة" لمُشغلي botnets .

ويتمكن محققوا مكافحة الجريمة الإلكترونية ومسؤولو تنفيذ القانون كثيراً من الحصول على تصريح قضائي بإغلاق مواقع الخداع والاحتيال عند تحديدها، ولكن يتم تصميم التمويه السريع تحديداً لتفادي جهود "الفصل" هذه من خلال زيادة صعوبة تتبع النشاط غير القانوني وتحديد موقعه الحقيقي.

ويستطيع أصحاب السجلات ومكاتب التسجيل خفض الممارسة من خلال طريقتين: (1) مراقبة نشاط DNS (سهولة اكتشاف التمويه السريع) وتقديم تقارير عن السلوك المشبوه إلى هيئة تنفيذ القانون أو أية آلية أخرى مناسبة لتقديم التقارير، و(2) تبني معايير تجعل التمويه السريع صعب التنفيذ أو غير جذاب. تتضمن بعض المعايير المحتملة التي تم اقتراحها:

- توثيق الاتصالات قبل السماح بإجراء تغييرات على سجلات NS،
- منع التغير الآلي في سجل NS،
- تنفيذ حد أدنى لـ "مدة الاستمرار" (TTL) لاستجابات طلب خادم الاسم[6]،
- تحديد عدد خوادم الاسم التي يمكن تحديدها لنطاق محدد، و
- تحديد عدد التغييرات في عنوان سجل (A) التي يمكن إجراؤها في إطار فاصل زمني محدد على خوادم الاسم المرتبطة بنطاق مُسجل.[7]

وفي الوقت الذي يتم فيه اقتراح هذه المعايير، يوصي الموظفون باستكشاف التضمينات الإضافية التي قد تتضمنها هذه المعايير. وينبغي الملاحظة أن عملية تطوير سياسة GNSO هي إحدى الطرق المتعددة التي قد تتناولها استضافة التمويه السريع داخل مجتمع ICANN. ويصف هذا القسم الآليات المتعددة لتناول هذه القضية بهدف إخبار مجتمع ICANN بالاتجاهات المحتملة التي يمكن اتخاذها.

[6] تم اقتراح 30 دقيقة كحد أدنى منطقي لمدة الاستمرار (TTL)، كما يُدرك الموظفون تنفيذ بعض المُسجلين مدة استمرار تصل إلى 30 دقيقة. وقد يتمكن مزودو الامتداد والمُسجلون من تحديد حالات الاستثناءات الخاصة بالاستخدامات القانونية لمدد الاستمرار (TTL) الأقصر، ولكن قد يكون من الصعب -من الناحية العملية- التمييز بين الاستخدامات القانونية والتطبيقات الضارة.

[7] من الممكن ألا تضرر الأنشطة القانونية من تحديد خوادم الاسم الخاصة بنطاق محدد بـ 5 خوادم، وتحديد عدد التغييرات بـ 5 تغييرات لكل شهر.

تطور وضع إرشادات أفضل الممارسات

يمكن أن يؤدي المزيد من المناقشة والبحث داخل المجتمع إلى تطوير مجموعة من الإرشادات الخاصة بوضع أفضل الممارسات. وفي نطاق ICANN، قد تُشكل هذه الإرشادات أساس الإجراءات التطوعية التي يقوم بها مزودو الامتداد والمُسجلون أو العمل بموجب عملية تطوير سياسة تالية أو المتطلبات التي يتم دمجها في عقود مزود الامتداد أو اتفاقيات اعتماد المُسجل. وخارج نطاق ICANN المباشر، يمكن تعزيز هذه الإرشادات بالنسبة لمقدمي خدمة الإنترنت ومُشغلي البنية التحتية للإنترنت الآخرين ومزودو الخدمة كإجراءات ومعايير مطلوبة بحيث يمكن التزامهم بها بشكل تطوعي.

وكما هو موضح في توصيات الموظفين (انظر القسم 5 والملخص التنفيذي في القسم 1)، يدعم موظفو ICANN رعاية المزيد من عمليات تحديد الحقائق والبحث لتطوير إرشادات أفضل الممارسات على أنها الخطوة الأولى التي ينبغي التزام GNSO بها.

عملية تطوير سياسة GNSO

قد تفرض توصيات السياسة الخاصة بهذه القضية مطالب جديدة أو تضع محظورات جديدة يمكن تطبيقها على الأطراف المتعاقدة، والتي سيقوم موظفو ICANN بتنفيذها وتفعيلها بعد ذلك من خلال عقود ICANN مع أصحاب السجلات و/أو مكاتب التسجيل. ومع ذلك، لا تستطيع ICANN سوى فرض التزامات جديدة على أصحاب السجلات ومكاتب التسجيل إذا كانت استضافة التمويه السريع تُمثِّل مشكلة "حيث تكون هناك ضرورة منطقية للحصول على قرار منتظم أو مُنسَّق لتسهيل القدرة على التشغيل والاعتماد الفني و/أو الاستقرار التشغيلي لخدمات مكاتب التسجيل أو خدمات أصحاب السجلات أو DNS أو الإنترنت". (اتفاقية اعتماد المُسجل (RAA) القسم 4.2.1)

5 توصيات الموظفين

كما تم ذكره بالتفصيل أدناه، يوصي الموظفون بقيام GNSO برعاية عمليات إضافية لتحديد الحقائق والمعلومات وعمليات بحث لتطوير الإرشادات المتعلقة بتنفيذ أفضل الممارسات فيما يتعلق باستضافة التمويه السريع. وقد يكون من المناسب مشاركة ccNSO أيضًا في هذا النشاط.

النطاق

وفي إطار تحديد ما إذا كانت المشكلة تقع داخل نطاق عملية سياسة ICANN ونطاق GNSO، قام الموظفون ومسؤولو المجلس العام بمناقشة العناصر التالية:

تحديد ما إذا كانت المشكلة داخل نطاق إعلان مهمة ICANN

تنص لوائح ICANN على:

"إن مهمة شركة الإنترنت للأرقام والأسماء المُخصصة ("ICANN") هي تنسيق نظام الإنترنت العالمي -على المستوى الكلي- للمعرفات الفريدة، وخاصة لضمان استقرار وأمان تشغيل نظم المعرفات الفريدة للإنترنت. وبشكل أكثر تحديداً، تقوم ICANN بـ:

1. تنسيق تخصيص المجموعات الثلاث من المعرفات الفريدة للإنترنت وتخصيصها، وهي
   أ. أسماء النطاق (تشكل نظاماً يشار إليه بـ "DNS")،
   ب. عناوين بروتوكول الإنترنت ("IP") وأرقام النظام المستقل ("AS ") و
   ج. منفذ البروتوكول وأرقام المعيار.
2. تنسيق تشغيل نظام خادم اسم الجذر لـ DNS وتطوره.
3. تنسيق تطوير السياسة التي تتعلق بهذه الوظائف الفنية بصورة منطقية وملائمة".

يتضمن التمويه السريع ارتباط أسماء النطاق بعناوين بروتوكول الإنترنت (IP) من خلال تشغيل خوادم الاسم، بما في ذلك المعلومات الخاصة بنطاقات المستوى الثاني التي تم تفويضها والتي يتم المحافظة عليها بواسطة مكاتب التسجيل وصاحب سجل ال TLD حيث يتم تسجيل SLD. تلتزم ICANN بمسؤولية محدودة فقط في عملية تطوير السياسة المتعلقة بهذه الوظائف الفنية. وفي الوقت الذي تكون فيه العناصر 1 أ و3 الواردة أعلاه بمثابة مواضيع عامة تقع داخل نطاق إعلان مهمة ICANN، لن يتم تطبيق بعض خيارات السياسة داخل نطاق وضع سياسة GNSO.

تحديد ما إذا كان من الممكن تطبيق المشكلة بشكل واسع على عدد من المواقف والمنظمات المتعددة

يمكن تطبيق الآراء المتعلقة بالقضايا المحيطة باستضافة التمويه السريع بشكل واسع على العديد من الأوضاع أو المنظمات المتعددة، بما في ذلك أي gTLD حالي ضمن عقد مع ICANN وكل من مكاتب التسجيل المعتمدة والبالغ عددها 800 وعدد من مسجّلي النطاق الحاليين والمحتملين. ولاحظ انه على الرغم من أنه يمكن فقط تطبيق سياسة الإجماع الناتجة عن عملية تطوير سياسة GNSO على أصحاب سجلات gTLD و مكاتب التسجيل الذين يعملون ضمن عقد مع ICANN (فقط في حالة أن تكون استضافة التمويه السريع بمثابة مشكلة "حيث تكون هناك ضرورة منطقية للحصول على قرار منتظم أو مُنسَّق لتسهيل القدرة على التشغيل والاعتماد الفني و/أو الاستقرار التشغيلي لخدمات مكاتب التسجيل أو خدمات أصحاب السجلات أو DNS أو الإنترنت". (اتفاقية اعتماد المُسجل (RAA) القسم 4.2.1)

تحديد ما إذا كان من المحتمل استمرار قيمة المشكلة أو سريانها، على الرغم من الحاجة إلى إجراء تحديثات أحيانًا

قد يؤثر إكمال عمل تطوير السياسة الخاصة بالمشاكل المتعلقة بموضوع استضافة التمويه السريع على أصحاب سجلات gTLDs و مكاتب التسجيل المستقبليين والأعمال المحتملة أو الهيئات غير التجارية التي لم تدخل إلى السوق بعد. ويجب توجيه اهتمام إلى كيفية تطوير خيارات السياسة ذات الفائدة الثابتة والتي لن يتم تحريفها بواسطة العوامل الضارة بشكل سريع.

تحديد ما إذا كانت المشكلة ستؤدي إلى وضع دليل أو إطار عمل لصنع القرار في المستقبل

يمكن أن تكون نتيجة عملية تطوير السياسة ذات قيمة مستمرة كما سبق، وذلك على الرغم من استمرار تطور الظروف الخاصة بالسوق، وهو ما سيؤدي بدوره إلى وضع إطار عمل لعملية صنع القرارات المتعلقة بالقضايا ذات الصلة في المستقبل.

تحديد ما إذا كانت المشكلة تتضمن إحدى سياسات ICANN الحالية أو تؤثر عليها

لا تتضمن المشكلة إحدى سياسات ICANN الحالية ولا تؤثر عليها تتوفر قائمة بسياسات الإجماع على الموقع http://www.icann.org/general/consensus-policies.htm.

وبناءً على ما سبق، يرى المجلس العام وجود بعض النواحي المتعلقة بموضوع استضافة التمويه السريع داخل نطاق عملية سياسة ICANN ونطاق GNSO. وبالنسبة لأنشطة استضافة التمويه السريع المتعلقة بـ gTLDs، فإن المشكلة تقع داخل نطاق GNSO ويجب تناولها. ومع ذلك، فإن السؤال الإجمالي حول كيفية تخفيف استخدام استضافة التمويه السريع في الجريمة الإلكترونية أوسع من عملية تطوير سياسة GNSO. ولن يتم تطبيق بعض الخطوات التي يمكن استخدامها لعدم تشجيع استضافة التمويه السريع أو إعاقتها، مثل الخطوات التي يمكن اتخاذها من قِبل مقدمي خدمة الإنترنت أو مستخدمي الإنترنت أنفسهم داخل نطاق وضع سياسة GNSO. وعلاوةً على ذلك، وعلى الرغم من استهداف استضافة التمويه السريع لـ gTLDs، غير أنه يمكن ملاحظة ذلك في ccTLDs. وبالإضافة إلى ذلك، يُعد السؤال الخاص بإمكانية أن تكون خيارات السياسة ذات "قيمة مستمرة أو سارية" ذا أهمية خاصة في سياق استضافة التمويه السريع، حيث من الممكن تقويض السياسات الثابتة بواسطة المجرمين الإلكترونيين الجسورين. وبناءً على المعلومات المتوفرة حتى الوقت الحالي، يقترح الموظفون دراسة الخيارات المحتملة لتطوير السياسة بشكل أكثر تفصيلاً. وستُوفر عمليات تحديد الحقائق الإضافية عمليات الاطلاع الضرورية لإخبار المجلس بشكل أفضل بخيارات السياسة المتاحة التي قد تكون أكثر فعالية. ويمكن أن تُوفر الخيارات المُفضَّلة بعد ذلك أساسًا لبدء تشغيل عملية محددة لتطوير السياسة.

الإجراء الموصى به

يوصي الموظفون بقيام GNSO برعاية عمليات إضافية لتحديد الحقائق والمعلومات وعمليات بحث لتطوير الإرشادات المتعلقة بتنفيذ أفضل الممارسات فيما يتعلق باستضافة التمويه السريع وتوفير البيانات للمساعدة في تطوير السياسة وإبراز خيارات السياسة المحتملة. وينبغي القيام بتطوير أفضل الممارسات بالتعاون بشكل واسع مع الأفراد ذوي المعرفة الكبيرة والمنظمات والمشاركة الواسعة لتشجيع المساهمة الكبيرة والتبني الواسع. ومن المحتمل قيام بعض المُسجلين بالفعل بتنفيذ بعض المعايير المحددة في SAC 025 كما يوصي الموظفون بإجراء مشاورات مع هؤلاء المُسجلين لتحديد مدى فعالية هذه المعايير والطريقة الأفضل لتطبيقها. ويمكن إتاحة موارد الموظفين لدعم هذه الأنشطة البحثية والأهداف.

وقد ركَّزت الدراسة التي قامت بها SSAC حول استضافة التمويه السريع بالإضافة إلى العديد من المقالات التجارية على الأسئلة الهامة التالية، بما في ذلك:

- من المستفيد من التمويه السريع، ومن يقع عليه الضرر؟
- من المستفيد من توقُّف الممارسة ومن سيقع عليه الضرر؟
- كيف اشترك مُشغلو مزود الامتداد في أنشطة استضافة التمويه السريع؟

- كيف اشترك المُسجلون في أنشطة استضافة التمويه السريع؟
- كيف تؤثر استضافة التمويه السريع على مسجّلي النطاق؟

تتضمن بعض الأسئلة الإضافية التي يمكن تناولها بشكل مفيد كجزء من تحديد الحقائق والمعلومات:

- كيف تؤثر استضافة التمويه السريع على مستخدمي الإنترنت؟
- ما هي القواعد الإجبارية التي يمكن تطبيقها لخفض الآثار السلبية لاستضافة التمويه السريع أو التخلص منها؟
- ما هو الأثر (الإيجابي أو السلبي) الذي سينتج عن وضع حدود أو إرشادات أو قيود على مكاتب التسجيل و/أو أصحاب السجلات فيما يتعلق بالممارسات التي تُمكِّن استضافة التمويه السريع أو تعمل على تسهيلها؟
- ما هي المعايير التي يجب تطبيقها من جانب أصحاب السجلات أو مكاتب التسجيل لتخفيف الآثار السلبية لاستضافة التمويه السريع؟ هل يجب توثيق هذه المعايير وتعزيزها كـ "وضع أفضل الممارسات"، ودمجها في عقود أصحاب السجلات واتفاقيات اعتماد مكاتب التسجيل أم ينبغي إعلانها بطريقة أخرى؟

التاريخ:
31 مارس 2008
(نص مُنقَّح)

اللغة العربية

الملحق 1 - طلب GNSO للحصول على تقرير مشاكل حول استضافة التمويه السريع

يُمثِّل هذا الملحق بالكامل طلب تقرير مشاكل تقدم به مجلس GNSO:

نظرًا للاستخدام المتزايد لتغييرات "التمويه السريع" لـ DNS لارتكاب الجرائم وإحباط جهود تنفيذ القانون في مكافحة الجريمة، ومع قيام المجرمين بتعديل عناوين بروتوكول الإنترنت (IP) و/أو خوادم الأسماء بشكل سريع في محاولة لتفادي اكتشافهم وإغلاق موقع الويب الإجرامي الخاص بهم،

ونظرًا لما قدمته اللجنة الاستشارية للأمان والاستقرار في هذا الشأن من خلال ورقة SAC 025 الاستشارية، بتاريخ يناير 2008. http://www.icann.org/committees/security/sac025.pdf/

ونظرًا لما تقوم به SSAC الاستشارية من وصف النواحي الفنية لاستضافة التمويه السريع وتوضيح كيفية استغلال DNS للتحريض على الأنشطة الإجرامية ومناقشة الطرق الحالية والمحتملة لتخفيف هذا النشاط، كما توصي بضرورة اتخاذ الأجهزة المعنية السياسات بعين الاعتبار، مما يجعل طرق التهدئة العملية متاحة على المستوى العالمي لجميع مسجّلي النطاق ومقدمي خدمة الإنترنت (ISP) ومكاتب التسجيل وأصحاب السجلات،

ونظرًا لإمكانية أن تكون GNSO طرفًا مناسبًا لمناقشة هذه السياسات

قرارات مجلس GNSO:

ينبغي على موظفي ICANN إعداد تقرير مشاكل فيما يتعلق بتغييرات "التمويه السريع" لـ DNS، بهدف قيام مجلس GNSO بمناقشته. وبشكل أكثر تحديدًا، ينبغي على الموظفين مناقشة ورقة SAC الاستشارية، وتوضيح الخطوات التالية المحتملة في تطوير سياسة GNSO والتي تم وضعها لخفض القدرة الحالية للمجرمين على استغلال DNS عبر "التمويه السريع" لعنوان بروتوكول الإنترنت (IP) أو تغييرات خوادم الأسماء.